Federal Election Commission
Washington, DC 20463

November 28, 2018

MEMORANDUM

TO: The Commission

THROUGH: Alec Palmer AP by MAH
Staff Director
Chief Information Officer

FROM: Katie A. Higginbothom KAH
Co-Chief Privacy Officer
Acting Deputy Staff Director for Management and Administration

Gregory R. Baker GRB
Co-Chief Privacy Officer
Deputy General Counsel - Administration

SUBJECT: Privacy & Data Protection Follow-Up Audit Updated Corrective Action Plan

The Privacy Team typically circulates to the Commission, on a biannual basis, an update to management's corrective action plan from the 2010 Privacy and Data Protection Follow-Up Audit. In March 2011, the Office of Inspector General issued its final audit report from the 2010 Privacy and Data Protection Follow-Up Audit, and on June 8, 2011, the Privacy Team circulated to the Commission management's Corrective Action Plan (CAP) to address the audit recommendations.

With the very recent hiring by the Administrative Law Team of an attorney with significant experience in handling Privacy Act-related matters, the Privacy Team now has additional staff resources to devote to addressing the CAP recommendations. With these additional resources, in the past 4 months the Privacy Team has closed out CAP recommendations 3B, 10B, 11A, 12A, and 13.

The Privacy Team intends to, among other things, continue to work to ensure that necessary privacy and security controls are fully instituted, and believe we can close out CAP recommendations 4A, 4B, 4C, 4D, 7A, 7D, 7E, 7F, 8D, 12B, 12D, and 12E in this fiscal year. Attached is an updated version of the corrective action plan provided for informational purposes.

Please feel free to contact the Co-Chief Privacy Officers if you have any questions.

Recommendation Title	Original Issue Date	Recommendation	Management Response	Project Summary Action	Estimated Implementation Date	Last Status Update	Revised Implementation Date	# of Days Open	Owner	Closure Opinion
Project Name: FY 2010 Follow-up Audit of Privacy and Data Protection										
Policy for Vendor Access to PII	3/31/2011	(11B) Should develop a policy and supporting procedures to assess and approve vendors with access to FEC PII to reasonably ensure that the vendor has adequate controls in place to protect the information before any PII is provided to the vendor.	Agree	Collaborate with the Contracting Officer and Chief Financial Officer to develop policies and supporting procedures that will require prospective contractors to provide evidence of internal controls that will safeguard the agency's sensitive information or PII that the contractor has access to.	9/30/2011	Contracting has developed a tracking spreadsheet to track vendors that handle PII and revised the COR responsibilities letter to include language which obligated the COR to alert the Contracting Officer to new contracts where vendors handle PII so that the Contractor can add the vendor to the spreadsheet. The revised COR letter and the tracking spreadsheet have been sent to the IG.	1/21/2019	-53	Katrina Sutphin	To verify policy implementation, the OIG requested the the most recent signed COR designation letter from the Contracting Officer. Upon review of a COR letter that was effective as of October 3, 2018, the updates proposed to resolve this item were not included in the letter. Management must make sure this corrective action has been implemented for all new contracts in order to sufficiently close this recommendation. See attachments included for Status update - 11/9/18 MF
Approval of Vendor Access to PII	3/31/2011	(11C) Should formally document the process used to review the FEC's vendors and the results should be retained to evidence the review procedures performed. In addition, there should be documented management approval from the department head that is the source of the information to be shared with the vendor and either of the co-Chief Privacy Officers before the vendor is provided access to FEC PII. There may be more than one department head that should review and approve a specific vendor if the PII affected pertains to more than one department.	Agree	Work with Contracting Officer to develop a process for reviewing and documenting vendor privacy controls. Create a CPO privacy approval process that vendors must undergo before gaining access to FEC PII. Evaluate various options for accomplishing this goal.	9/30/2011	Work with Contracting Officer to document or develop a process for reviewing and documenting vendor privacy controls.	11/1/2019	-337	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Timely Updates to SORs	3/31/2011	(12B) Enhance existing guidelines and procedures to include timelines and deadlines that promote regular review and timely updates to SORs.	Agree	Update the SORNs Review Guidelines and the Procedures for Conducting the Circular A-130 System of Records Notices Review to include internal benchmarks and goals for biennial reviews and updates of SORNs and SORs.	1/31/2012	OGC has agreed to a biennial (every 2 years) review of the SORs which the privacy attorney will be conducting by March 31, 2019. This review as a matter of course will include all FEC departments including the Physical Security Officer, the FEC Records Officer, and FEC Management, Facilities, and every area of the FEC. The policy that states we will conduct this review every two years was sent to the IG as was the SOR 'checklist' which tells us in total what SORs we currently have. After the policy you will find the form we intend to fill out for each SOR to ensure the SOR has been properly reviewed	5/1/2019	-153	Katrina Sutphin	The OIG reviewed management's status update to conduct a review by March 31, 2019. Once the review is conducted, the OIG will be able to assess the results of the corrective actions taken. Until that time, the recommendation remains open. The OIG revised the implementation due date to correlate with management's stated review period. 11/9/208 - MF
SORs Assessment of electronic and paper records	3/31/2011	(12D) Work with the Physical Security Officer, the FEC Records Officer, and FEC management to incorporate SORs assessment processes into electronic and paper records management processes.	Agree	Work with the Administrative Services and the Commission Secretary's Office to ensure that SORs are considered during records management and physical security operations.	3/31/2012	OGC has agreed to a biennial (every 2 years) review of the SORs which the privacy attorney will be conducting by March 31, 2019. This review as a matter of course will include all FEC departments including the Physical Security Officer, the FEC Records Officer, and FEC Management, Facilities, and every area of the FEC. The policy that states we will conduct this review every two years was sent to the IG as was the SOR 'checklist' which tells us in total what SORs we currently have. After the policy you will find the form we intend to fill out for each SOR to ensure the SOR has been properly reviewed	5/1/2019	-153	Katrina Sutphin	The OIG reviewed management's status update to conduct a review by March 31, 2019. Once the review is conducted, the OIG will be able to assess the results of the corrective actions taken. Until that time, the recommendation remains open. The OIG revised the implementation due date to correlate with management's stated review period. 11/9/208 - MF
Policy for Monitoring and Reporting SORs	3/31/2011	(12E) Develop and implement policies and procedures that define monitoring and reporting processes to ensure SORs are updated and amendments published in accordance with Federal regulations by: 1) providing regular training to FEC managers and SOR system owners/managers; 2) establish deadlines, based on the legal requirements of OMB A-130, for documenting the new SORs, revisions to existing SORs, and publish the updated SORN; 3) providing legal assessment of potential changes in SORs and quality assuring the SORs produced by system owners/managers; 4) including performance standards in employee performance plans that are linked to successful compliance with Federal regulations; and 5) requiring regular reporting of compliance with the timelines to the Commission.	Agree	Develop privacy system manager training. Create internal benchmarks or goals to meet SORNs publication deadlines. Continue conducting legal assessments of potential system of record changes.	3/31/2012	Send a memo to FEC managers explaining the institution and use of the SOR addition form and requesting any SOR additions by Dec 2018. By March 31, 2019, the privacy counsel will conduct the first biennial SOR review and update the SORs for the FEC. After this first review, the privacy team will continue conducting legal assessments of potential system of record changes and also will accept submissions of SORs using the SOR addition request form from managers outside the Privacy Team. A record of the Biennial SOR reviews will be kept for the IG to review. Privacy Counsels standards include reference to keeping accurate records and reviewing departments for changes.	1/21/2019	-53	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Privacy Impact Assessments	3/31/2011	(2A) Conduct privacy impact assessments in accordance with Section 522, or create an alternative process for ensuring that privacy risks associated with PII are documented, assessed and remediated as necessary.	Agree	Create a privacy impact evaluation process to track the information collected in, and system controls for, information systems.	11/30/2011	OCFO has an ERM process in development per the new A123 guidance that assesses risk agency-wide and could cover this recommendation. Privacy Counsel will meet with Gilbert and discuss, then provide further action plan. Management is researching and developing a solution to address the recommendation.	12/1/2019	-367	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Compliance with OMB guidance	3/31/2011	(2B) Comply with OMB memoranda, or in the event of statutory exemption and a decision not to voluntary comply, document that sufficient controls exist to mitigate the need to comply. Where compliance is not adopted due to resource constraints or other reasons, document the legal assessment, risk analysis, and cost-benefit to the FEC.	Agree	Conduct an informal cost-benefit analysis of privacy-related OMB requirements when the agency is exempt from such requirements.	9/30/2011	Management is researching and developing a solution to address the recommendation	12/1/2019	-367	Katrina Sutphin	Will review management's planned corrective action once identified.
Governance Framework to Protect PII	3/31/2011	(2C) Identify and implement a governance framework (e.g., NIST, the AICPA's Generally Accepted Privacy Principles (GAPP)), to ensure that controls within the FEC to protect PII are appropriately identified, documented, and implemented.	Agree	Review the AICPA Generally Accepted Privacy Principles (GAPP) and determine it is feasible to implement as a privacy governance framework for the agency, in whole or in part.	4/30/2012	Management is researching and developing a solution to address the recommendation.	12/1/2019	-367	Katrina Sutphin	Will review management's planned corrective action once identified.
Inventory of Systems with PII	3/31/2011	(4A) Update and maintain the inventory of all systems that contain PII for all the divisions. A potential approach is to use the templates created by STSI and have each division update their current listing and implement business processes to continually update the inventory based on new or revised handling and storage of PII. A full review could be conducted by the divisions at least annually and would help support the biennial Privacy Act Systems of Records update process.	Agree	Update the 2009 PII review inventory. Note: These action items are subject to the availability of contractor funds and Commission notification.	4/30/2012	Update the 2009 PII review inventory and provide proof of this procedure to the IG.	2/1/2019	-64	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.

FEC Management Document

CAP of STSI recommendations	3/31/2011	(4B) Finalize the evaluation of the draft STSI recommendations and develop, document and implement a corrective action plan as necessary. Progress against the corrective action plan should be formally and periodically reported to management.	Agree	Complete review of evaluation report recommendations, approval of the recommendations, and prepare an action plan for addressing the approved recommendations.	2/29/2012	Review STSI report, notate on report which action items correspond to the CAP and refer IG to the current CAP plan to resolve those joint STSI and CAP audit items. If any items on the STSI plan do not correspond to the CAP plan these will be addressed and resolved. This document will be provided to the IG.	1/21/2019	-53	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
SSN Reduction Plan	3/31/2011	(4C) Provide the Privacy Team's SSN Reduction Plan Phase 1 report to the applicable division heads, and work with those offices to prepare action plans to address the findings in the report.	Agree	Approve the SSN Reduction Plan Phase 1 report and work with division heads to address the report findings.	3/31/2012	Audit and inventory Social Security Number and PII usage within FEC. Interview information owners and determine whether PII and SSN collection and storage is necessary. Prepare spreadsheet reporting those findings to IG. (4c) Remediate by eliminating unnecessary uses of PII and SSNs (4d) and reporting results to IG. This process will be completed once per fiscal year. A record will be kept noting that we completed this process each year.	2/1/2019	-64	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Comply with OMB M-07-16	3/31/2011	(4D) Complete Phase 2 and Phase 3 of the "FEC's Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers in Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" as soon as practical. This can be accomplished by providing the STSI results to the divisions and requesting a response on the ability to reduce or eliminate the questionable uses of social security numbers already identified by the contractor.	Agree	Complete Phases 2 and 3 of the plan by disclosing the findings of the Phase 1 report to the applicable division heads, and work with division heads to address the report findings.	3/31/2012	Audit and inventory Social Security Number and PII usage within FEC. Interview information owners and determine whether PII and SSN collection and storage is necessary. Prepare spreadsheet reporting those findings to IG. (4c) Remediate by eliminating unnecessary uses of PII and SSNs (4d) and reporting results to IG. This process will be completed once per fiscal year. A record will be kept noting that we completed this process each year.	2/1/2019	-64	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Annual Risk Assessment of Systems with PII	3/31/2011	(5A) Conduct a risk assessment annually for all existing and new applications that collect, process, transmit or store PII. If PIAs were performed, a risk assessment component could be built into that process to accomplish both the PIA and risk assessment recommendations.	Agree	Conduct an informal risk assessment of agency PII during the biennial PII Review. Note: These action items are subject to the availability of contractor funds and Commission notification or approval.	5/31/2012	Conduct an informal risk assessment of agency PII. This could possibly be resolved with Gilbert's risk mgt process further research needed.	12/1/2019	-367	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Develop CAP for risk assessment deficiencies	3/31/2011	(5B) Prepare a documented corrective action plan for any deficiency noted for each risk assessment performed and report progress periodically until all corrective actions are implemented. The corrective action plan should be approved by management.	Agree	Prepare an informal documented assessment of the findings from the next biennial PII review, with recommended action items. Note: These action items may be subject to the availability of contractor funds for the 2011 PII Review.	9/30/2012	Prepare a corrective action plan for what is found in 5A.	12/1/2019	-367	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Identification of Encrypted Devices	3/31/2011	(6E) Include a record in the inventory listing of whether the device is encrypted or not.	Agree	Management does not concur with this recommendation and refers to its response in the final audit report.	9/30/2011	Management will provide a report that shows that devices are encrypted.	2/1/2019	-64	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Regular Privacy Walkthroughs	3/31/2011	(7A) ISSO, Physical Security Officer, and/or division management should conduct regular walkthroughs to ensure that agency staff complies with privacy and information security standards are being met. Implementation of these action items are subject to Commission notification and/or approval.	Agree	ISSO, Physical Security Officer and other management officials as appropriate will conduct walkthroughs of the building to ensure privacy and information security standards are being met. Implementation of these action items are subject to Commission not	9/30/2011	Create a policy to conduct yearly walkthroughs to ensure staff comply with privacy and information security standards. Document findings. Make log documenting yearly walkthroughs available to IG for inspection.	12/1/2018	-2	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Address Failures to Secure Sensitive Information	3/31/2011	(7D) Division managers should work with the Physical Security Officer and the Records Officer to assess records management and secure storage needs and address failures to adequately secure sensitive information noted during the walkthrough.	Agree	Discuss with the Physical Security Officer and the Records Officer security concerns for storage areas and records management raised during the security walkthroughs. Include in the discussion the pros and cons of locking suite doors after business hours. Implementation of these action items are subject to Commission approval if the security walkthroughs.	9/30/2011	Resolve issues found in walkthrough. Include in the discussion the pros and cons of locking suite doors after business hours.	7/1/2019	-214	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Contractor Certification of Secure Destruction	3/31/2011	(7E) Contracting Officer and COTRs should enforce the requirement for contractors to certify secure destruction or return of FEC information in both paper and electronic format	Agree	Assist the Contracting Office in developing a process for ensuring contractors return or securely destroy FEC information when no longer needed.	9/30/2011	Create and institute an exit checklist for contracts that are ending that ensures that contractors return or securely destroy FEC information when no longer needed.	12/1/2018	-2	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
COR Policies	3/31/2011	(7F) Should establish policy and procedures requiring COTRs to inspect the physical space occupied by contractors when the contractor departs to ensure paper and electronic records are securely disposed of or filed	Agree	Work with the Contracting Officer to develop policies and procedures regarding COTR inspection of contractor-occupied space after termination of the contract.	9/30/2011	Create and institute an exit checklist for contracts that are ending that includes an inspection of contractor-occupied space after termination of the contract.	12/1/2018	-2	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.
Annual Review of Privacy Policies	3/31/2011	(8D) Should review on a regular basis all of the privacy and data security policies, procedures, standards and guidelines on a defined timeframe (e.g., annually), and they should be dated, and updated as necessary and include a point of contact if employees have questions.	Agree	Conduct a biennial review of the privacy policies and continue the annual review of IT security policies. As part of these reviews, ensure that the policies contain a point of contact and effective and revision dates.	3/31/2012	Conduct and keep a log of annual reviews of all privacy policies. Make log available to IG for inspection. The first privacy inspection will be conducted April 2019	10/30/2019	-335	Katrina Sutphin	Reviewed management's updated corrective action plan and will assess the adequacy of implementation once completed.